King County
Elections

Records, Elections and Licensing Services Division
Department of Executive Services

Criteria to Determine Successful Testing of Upgraded Vote Tabulation Solution as Required by Motion 2007-0402 (F)

In order to ensure that the upgraded vote tabulation system functions as documented and promised by the vendor and provides the required security measures to ensure public trust and confidence, King County Elections plans a four phase testing program. This test program is based on best practices used in other county IT projects such as the Disabled Accessible voting Equipment project (DAVE) and testing practices utilized in other counties and states including the California top-to-bottom review. Specific details concerning each test are still under development as Elections works with experts in the field, proposed vendor, other elections entities, Council staff, and OIRM.

The phases and purpose of each phase includes:

- Delivery acceptance testing of the equipment and software to determine if the correct model and versions of the equipment and software are delivered and that the equipment, software and system operate as documented by the vendor.
- Mock election to ensure that the equipment, software and system perform each of the functions required by federal, state and local law in order to administer an election from the beginning to the end.
- Volume/stress testing to ensure that the equipment, software and system will standup to the maximum expected volume for our largest election as well as the system's ability to handle the unexpected such as an unexpected peak in adjudication activity. This will be done by exercising the system with 50 percent more volume than expected and evaluating system performance. It will highlight if the equipment is properly sized in CPU capacity, system memory, etc. to meet Elections needs without crashing, unacceptable performance degradation or compromising the integrity of the system. It will also provide a measurement of the systems ability to handle the inevitable growth in voter registration over the life of the system (six – eight years). For instance, this type of test would help identify whether there would be any database size issues such as those experienced with the current system.
- Security review to ensure examination by third party information technology security experts beyond the federal certification process and provide confidence that any security risks are identified and mitigated.

The standard for success for each testing phase, and for all testing phases cumulatively, will be compliance with the identified measures of success. These criteria may need to be modified as the testing plan is developed further and as Elections' personnel learn more about the specific equipment and software.

Criteria or Measures of Success for each Phase shall be:

Delivery acceptance testing of the equipment and software done from a checklist

- All hardware and software components were delivered, installed and are available for testing according to contract terms.
- All models and model numbers match the contract and other documentation.
- The software versions are those that have been certified at the federal and state level and agreed to by the County and the vendor.
- No hardware components are damaged.
- No software components are corrupted.

Pursuant to state law any model or version numbers not matching the federally certified system will not be accepted. Any damaged hardware components will be repaired or replaced by the vendor and any corrupted software will be replaced by the vendor. Before beginning the next testing phase, the delivery acceptance testing of each hardware and software component shall be completed.

The security review which shall be conducted in parallel with the Mock Election and Volume/Stress testing shall not begin until completion of delivery acceptance testing.

Mock Election

All hardware and software components required in order to conduct an election in King County function as documented by the vendor, both individually and in concert with all other existing and new hardware and software components, in a real election environment simulating a Primary Election, from the beginning of the elections process to final tally, accounting and certification.

If a hardware or software components do not function as required by federal and state law or as documented by the vendor and the issue can not be resolved, or a system wide failure requires the restart of the mock election then the system shall not be accepted pursuant to the contract. The next phase of testing shall not commence until each phase of the mock election has been successfully completed.

Volume/Stress Testing

- The equivalent of 1.5 million previously folded ballots can be scanned, processed and tallied in a timely manner and without failure of the hardware or software or extraordinary human intervention. The actual number of ballots may vary based on normally accepted methods of scaling in tests (e.g. rather than 1.5 million ballots on 15 scanners 30,000 ballots on 3 scanners and replicating the data)
- The system processes ballots printed by the primary print vendor as well as 5% of the total number of ballots that will have been printed by an alternate print vendor. The requirement for a mixture of print vendors ensures that the system functions properly independent of print vendors.
- The system imports, processes and counts 100,000 additional ballots from Accessible Voting Units (AVU) to ensure integration through the range of tabulation methods
- The system processes the following volume of ballots in each category:

- 30,000 (2% of total) ballots with write-in votes; 15,000 (1% of total) ballots with overvotes; 500,000 (33.3% of total) ballots with undervotes; 200 totally blank ballots.

The system must be capable of handling this volume of ballots to be acceptable pursuant to the contract.

Security Review

The system will be deemed acceptable if:

- Any security vulnerabilities identified by information technology security experts can be mitigated by implementation of administrative policies, procedures and processes; are detectable through normally employed procedures; or are of a magnitude deemed to be highly improbable or of insignificant consequences.
- Warning notifications through printable documentation like audit logs are available and effective to alert election administrators of any attempt at unauthorized access or intrusion into the system.

In the event a probable or significant security vulnerability is identified that can not be mitigated through administrative policies, procedures or processes or a warning notification is not available to detect an identified attack the system shall not be accepted pursuant to the contract.